UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/559,767	03/16/2006	Roberto Avanzi	DE030202US1	5670

65913 7590 02/09/2010

NXP, B.V.
NXP INTELLECTUAL PROPERTY & LICENSING
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
02/09/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 10/559,767	**Applicant(s)** AVANZI, ROBERTO	
	Examiner SHEWAYE GELAGAY	**Art Unit** 2437	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 25 January 2010 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1-13*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

Continuation of 11. does NOT place the application in condition for allowance because: Applicant's argument with respect to the rejection of the claims over the combination of Coron and Lauter has been considered but are not persuasive. The applicant argued that "claim 1 is patentable over the proposed combination of Coron and Lauter because the reasoning in the Office Action is not rational and, hence, is insufficient to establish prima facie case of obviousness." Examiner respectfully disagrees. Coron teaches resistance against "Differential Power Analysis" (DPA) for Elliptic Curve cryptosystem by providing countermeasure that thwart the attacks that enable to recover the private key stored inside the smart-card. Specifically, they teach three countermeasures that prevent from the attack such as randomization of the private exponent, blinding the point P and randomized projected coordinates. And Lauter teaches a cryptosystem based on a Jacobian of a hyperelliptic curve is being used. Typically, the curve-based cryptosystem is based on a group whose size is known to the cryptosystem designer but unknown and believed difficult to determine for attackers of the cryptosystem wherein the encryption and decryption that uses keys that are generated based on aspects or characteristics of a mathematical hyperelliptic curve. This exemplary cryptosystem is based on the Jacobian of the hyperelliptic curve being used, and the secret group size is the size of the group points on the Jacobian curve. The cryptosystem is described primarily with respect to generation of a "short" signature or product identifier which is code that allows validation and/or authentication of the machine, program user, etc. The signature is a "short" signature in that it uses a relatively a small number of characters. Lauter teaches that encryption and decryption are performed in cryptosystem based on secret, which is the size of of the group of points on the Jacobian of a hyperelliptic curve. The hyperelliptic curve can have genus greater than or equal to two. However, in certain implementations the curve may be elliptic curve (e.g. a hyperelliptic curve having genus equal to one). The applicant further argued that "the stated advantage comes from the secondary reference and specifically refers to advantages of elliptic curve cryptography technique compared with a conventional RSA method, which does not appeal to be an elliptic or hyperelliptic technique. Thus, the stated advantage is not related to the proposed modification using the hyperelliptic technique within an elliptic system." Examiner would like to point out that Lauter teaches the benefit of utilizing higher genus curves, e.g. hyperelliptic curves (based on a Jacobian of the hyperelliptic curve) with genus greater than or equal to two that would likely improve the security of the public key cryptosystem. The combination of Coron and Lauter teaching is consistent with the Applicant's teaching described on paragraph [0014] "the present invention is based on the principle of providing counter-measures for defence against attacks based on DPA in the implementation of hyperelliptic cryptosystems, and in particular that of scalar multiplication on the Jacobian variation." It would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Coron with Lauter in order to provide advantage of improved security while requiring shorter key lengths. (col. 2, lines 15-35; Lauter) Applicant's argument with respect to the rejection of the claims 1 and 8 over the combination of Joyce in view of Lauter is persuasive and the rejection of claims 1 and 8 has been withdrawn.The examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992)